

SYSTEM AND METHOD OF DYNAMIC KEY GENERATION  
FOR DIGITAL COMMUNICATIONS

ABSTRACT OF THE DISCLOSURE

An encryption system and method for generating encryption keys between  
5 sender and receiver for a symmetric-key encryption system begins with an initialization  
step on both ends of the communication channel, in which a initialization string is  
exchanged between sender and receiver by secure methods. Thereafter, a pseudo-  
random-function generator operating on the initialization string is used to generate a  
master recovery key at both ends. The master recovery key is operated on by a  
10 succession of pseudo-random-function generators to produce an encryption key, which  
is used to encrypt data at the sender, creating ciphertext, and decrypt at the receiver.  
After a block of ciphertext is transmitted and received, a new encryption key is  
generated by subjecting the master recovery key to another pseudo-random-function,  
and adding entropy by means of still another pseudo-random function operating on the  
15 current ciphertext. The method also provides error correction and detection on two  
levels, detecting transmission errors on one level, and loss of synchronization on  
another level. Errors in synchronization without errors in transmission are used to  
detect intrusion by unauthorized communications.